Control Number : TAC-16-35997

JUSTIFICATION FOR AN EXCEPTION TO FAIR OPPORTUNITY

1. Contracting Activity: Department of Veterans Affairs (VA)
Office of Acquisition Operations
Technology Acquisition Center
23 Christopher Way
Eatontown, NJ 07724

2. Description of Action: The proposed action is for a firm-fixed-price delivery order (DO) to be issued under the National Aeronautics and Space Administration (NASA) Solutions for Enterprise-Wide Procurement (SEWP) V Government Wide Acquisition Contract (GWAC) for a brand name International Business Machines (IBM) Security QRadar Core Appliance and associated hardware and software maintenance services.

3. Description of Supplies or Services: VA, Office of Information and Technology, Service Delivery and Engineering, Enterprise Operations (EO), in support of VA's Continuous Readiness Information Security Program (CRISP), requires a brand name IBM Security QRadar Core Appliance and associated hardware and software maintenance services. The IBM QRadar requirements shall provide for system security monitoring of VA network system logs and connectivity to provide security event and log correlation, security event alerts, information security threat intelligence, and reporting of all malware activity. VA uses a Security Information and Event Management (SIEM) solution for security monitoring of data center systems and networks. The SIEM remote processors and data collectors centralize all security incident event information for visibility from a management console for a central view of all SIEM event management and alerting activities. VA requires a technical refresh and upgrade of the current brand name IBM QRadar production event processors supporting the SIEM solution before they reach end-of-life, in addition to hardware and software maintenance services. The required refresh and upgrade will provide for increased event monitoring and flow capacity capabilities and will integrate with the current brand name IBM QRadar architecture and infrastructure supporting EO that includes IBM QRadar consoles, IBM QRadar licensing, and associated IBM QRadar event collector and processors for central QRadar device management, event reporting, event alerting, and event correlation. The QRadar SIEM architecture monitors, alerts, correlates, and provides information technology (IT) security threat intelligence for all data processed by systems managed by EO, including collected network flow information. Successful completion of this refresh requires the purchase of one IBM Security QRadar Core Appliance and the associated hardware and software maintenance services. The required hardware and software maintenance services shall consist of minor updates, patches, fixes, and security resolutions developed by IBM. The hardware and software maintenance services shall also consist of the analysis, troubleshooting, and resolution of any product-related problems 24 hours per day, 7 days per week, 365 days a year via telephone, email, or web-based portal. The total estimated value of the proposed action is REDACTED, which includes delivery of the required appliance within 30 days of DO award and 12-months of hardware and software maintenance services.

4. Statutory Authority: The statutory authority permitting an exception to fair opportunity is Section 41 U.S.C. 4106(c)(2) as implemented by the Federal Acquisition Regulation (FAR) Subpart 16.505(b)(2)(i)(B), entitled “Only one awardee is capable of providing the supplies or services required at the level of quality required because the supplies or services ordered are unique or highly specialized.”

5. Rationale Supporting Use of Authority Cited Above: Based on market research, as described in section eight of this document, it was determined that limited competition is available among authorized resellers of the required brand name IBM QRadar Core Appliance and associated hardware and software maintenance services. Only a brand name IBM appliance and associated hardware and software maintenance services can meet all of the Government’s requirements. EO previously acquired and currently uses IBM QRadar appliances throughout its SIEM architecture and infrastructure. Since the current VA SIEM architecture and infrastructure consists solely of IBM products, any appliances used to expand upon the architecture and infrastructure must be capable of integrating and interoperating with the currently owned brand name IBM products. The IBM QRadar appliance is a dedicated piece of IBM QRadar hardware incorporating the IBM QRadar security software. Thus, the term appliance refers to the integrated QRadar hardware and software security solution. The brand-specific functionality that this appliance supports in the existing overall architecture includes security event processing, network flow processing, metadata communication, data de-duplication, data encryption, data compression, risk management, and internal data and event correlation. If an alternative appliance were introduced to this environment, there would be interoperability and compatibility issues with the current QRadar (SIEM) architecture and infrastructure. Any other brand name appliance would require an extensive re-development effort to replace the current EO SIEM architecture and infrastructure as the appliance hardware and software components are proprietary to IBM. If another brand name appliance were used, it would not be interoperable or compatible with the existing security appliance infrastructure. Furthermore, VA IT Security Specialists estimate it would require approximately two years to replace the current QRadar SIEM production architecture and infrastructure. Only hardware and software maintenance services provided by IBM or an authorized reseller can meet the requirements as the existing hardware and software is proprietary to IBM. Specifically, without access to IBM’s proprietary source code, no other source is able to provide minor updates, patches, fixes, or security resolutions. Without the required hardware and software maintenance services, the existing SIEM appliance architecture and infrastructure performance would eventually degrade and would not be usable by EO as its system security monitoring solution. In addition, VA would not receive security updates, which could compromise VA’s entire network security posture. Additionally, since the hardware and software is proprietary, no third party source exists that provides analysis, troubleshooting, and resolution of any appliance-related problems other than IBM or an authorized IBM reseller.

6. Efforts to Obtain Competition: Currently, no other companies other than IBM or an authorized reseller can provide the required QRadar Core Appliance and hardware and software maintenance services. Market research was conducted, details of which are in section eight of this justification. This effort did not yield any additional sources that can

meet the Government's requirements. It was determined however, that limited competition is viable among authorized resellers for this brand name software maintenance and support. In accordance with FAR 5.301 and 16.505(b)(2)(ii)(D), notice of award of this action will be synopsized and this justification will be made publicly available on the Federal Business Opportunities Page within 14 days of award. This justification shall also be posted with the solicitation on the NASA SEWP V website for review by prospective offerors.

7. Actions to Increase Competition: The Government will continue to review and revalidate its requirements as security monitoring technology and solutions continue to evolve. The requiring activity will continue to research and monitor whether there are emerging products that enter the marketplace that are interoperable and compatible with EO's current SIEM architecture and will monitor other new security monitoring appliance product offerings to determine if an entirely new solution could technically and cost-effectively meet VA's future requirements.

8. Market Research: Market research was conducted by VA technical experts as part of a continuous process beginning September 2014 through July 2016. The market research was conducted by a review of industry websites and analysis of similar SIEM products offerings. This included a review to confirm if other brand name products, including those from Intel Corporation's Intel Security; EiQnetworks Inc.; Trustwave Holdings, Inc.; and Splunk, Inc. could meet the Government's functional and technical requirements. The review determined that other sources cannot provide SIEM appliance products that are interoperable and compatible with VA's existing QRadar hardware and software infrastructure. VA Subject Matter Experts regularly review industry trade publications and conduct internet research to ascertain if any other SIEM solutions are available which could be interoperable and compatible with the existing architecture and infrastructure. Based on the market research, the Government's technical team concluded that only a brand name IBM Security QRadar Core Appliance can provide for the required appliance and associated hardware and software maintenance refresh and upgrade to increase VA's security event and network flow capacity capabilities.

Additionally, these vendors cannot provide the required IBM hardware and software maintenance services because these vendors cannot access the source code and technical data of the proprietary IBM QRadar hardware and software architecture. Each source offers a proprietary system and associated maintenance services that will only operate with its respective hardware and software. An alternative SIEM solution would also require proprietary hardware and software maintenance which would not resolve the inability to obtain hardware and software maintenance services from vendors other than through the respective providers. Based on this market research, only an IBM Security QRadar Core Appliance and associated hardware and software maintenance services can meet VA's technical requirements.

Additional market research was conducted in July 2016 by utilizing the NASA SEWP V Market Research Tool. It was determined that there are numerous NASA SEWP V GWAC holders that are authorized resellers that can provide the required IBM Security

QRadar Core Appliance and associated hardware and software maintenance services. under North American Industry Classification System code 541519. Therefore, limited competition is anticipated for the requirements described herein.

9. Other Facts: None.